IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Criminal No. 2:23-cr-20191-MSN**
	)	
JUSTIN SMITH, *et al.*,	)	
	)	
Defendants.	)	

UNITED STATES' NOTICE OF INTENT TO INTRODUCE SELF-AUTHENTICATING DIGITAL MATERIALS – EXTRACTION OF DEFENDANT TADARRIUS BEAN'S PHONE

The United States submits this notice of intent to introduce self-authenticating materials from defendant Tadarrius Bean's cell phone, pursuant to Federal Rule of Evidence 902.

Under Rule 902, certain evidence is self-authenticating. Specifically, Rule 902(14) provides that evidence is self-authenticating if it is:

> Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Fed. R. Evid. 902(14). In enacting Rule 902(14), the Advisory Committee on Proposed Rules noted that, "[a]s with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing an authenticating witness for this evidence is often unnecessary." Fed. R. Evid. 902, Committee Notes on Rules—2017 Amendment. Because "[i]t is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented," Rule 902(14) "provides a procedure

in which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly." *Id.*; *see also United States v. Dunnican*, 961 F.3d 859, 872 (6th Cir. 2020) (discussing Rule 902(14)).[1]

In this case, defendant Bean voluntarily provided his phone, an Apple iPhone 13, to the Tennessee Bureau of Investigation (TBI) and signed a consent to search. TBI examined the phone using forensic extraction software.[2] The government intends to introduce evidence extracted from the device, including text messages, at trial, which is scheduled to begin on September 9, 2024.

Attached to this notice is a signed certification from Tennessee Bureau of Investigation Special Agent Derek Miller, who conducted the extraction of data from the phone. In the certification, TBI SA Miller attests that he is qualified to conduct the extraction and that the process used to do so was reliable.

Respectfully submitted,

KEVIN G. RITZ
United States Attorney

DAVID PRITCHARD
ELIZABETH ROGERS
Assistant United States Attorneys
167 N. Main Street, Ste. 800
Memphis, TN 38103

KRISTEN CLARKE
Assistant Attorney General
Civil Rights Division
U.S. Department of Justice

By: s/ Andrew Manns
FORREST CHRISTIAN
Deputy Chief

[1] The content of this notice and the attached affidavit are based on the same notice and affidavit provided in *Dunnican*. The Sixth Circuit specifically approved of a nearly identical notice and its contents in affirming the lower court's ruling that the phone materials were authentic.

[2] The Federal Bureau of Investigation (FBI) applied for and was issued a separate search warrant for the content of the phone on February 3, 2023. That warrant was executed on February 7, 2023.

KATHRYN E. GILBERT
Special Litigation Counsel
ANDREW MANNS
Trial Attorney
950 Pennsylvania Ave., NW
Washington, DC 20530

CERTIFICATE OF SERVICE

I, Andrew Manns, hereby certify that on the date below, I electronically filed the foregoing with the Clerk of Court for the Western District of Tennessee via the Electronic File System, which sent notification of said filing to defense counsel.

s/ Andrew Manns
ANDREW MANNS
September 6, 2024

CERTIFICATE OF AUTHENTICITY OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIUM, OR FILE, PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(14)

I, TBI Special Agent Derek Miller, attest and certify, under penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct.

1. I am employed by the Tennessee Bureau of Investigation (TBI), and my title is Special Agent. I have been employed by TBI since approximately 2014. As a Special Agent with TBI, I have extensive training and experience in extracting data from mobile devices. I have received technical and computer-related training in the following courses: Digital Evidence Acquisition Specialist Training Program (DEASTP), Seized Computer Evidence Recovery Specialist (SCERS), SANS Security Essentials (GSEC), Digital Currency Course and numerous other courses at the National Computer Forensics Institute provided by the United States Secret Service, multiple courses taught by creators and vendors of digital forensic examination tools, and many other courses involving the investigation of computer systems and other technologies. In the course of my career, I have made approximately 600 forensic images and extractions of digital devices, including images of mobile devices such as cellular phones.

2. I am qualified to authenticate the digital extraction referenced in this certificate because of my experience and training and because I created the digital extraction listed below:

Original Device	Source	Date of Image	Extraction Identifier
Apple A2484 cell phone; IMEI 359836511755757	Consent to Search from Tadarrius Bean, signed January 23, 2023	January 24, 2023	JA20230014

3. The extraction described above is a true duplicate of the original device.

4. The extraction identified above was made at or near the time the content from the device was seized, using specialized forensics software, called Graykey. In my training and experience, this forensic software creates an accurate and reliable extraction of digital mobile devices at the moment in time in which the extraction is performed, and I have regularly relied on Graykey to create an accurate and reliable extraction in the past.

5. Further, I know that the forensic extraction process was complete and accurate because the forensic software generated a hash (i.e., a digital fingerprint) of the extracted data and because the software expressly indicated that the extraction was successful.

I further state that this certification is intended to satisfy Rules 902(11) and 902(14) of the Federal Rules of Evidence.

9/6/2024
Date

Derek Miller
Special Agent
Tennessee Bureau of Investigation